UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/376,384	08/16/1999	GERSHON BAR-ON	U013169-9	6449

140 7590 07/19/2004

LADAS & PARRY
26 WEST 61ST STREET
NEW YORK, NY 10023

EXAMINER	
SEAL, JAMES	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 07/19/2004

15

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/376,384	BAR-ON, GERSHON	
	Examiner	Art Unit	
	James Seal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *52-78,80-86 and 88-95* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *52-78,80-86 and 88-95* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 02 April 2004.

2. The change of inventorship under 37CFR 1.48 (b) has been approved.

3. Claims 1-51, 79 and 87 have been cancelled with without prejudice.

4. New claims 89-95 have been entered

5. Claims 52-78, 80-86, and 88-95 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 55 and 56 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular in both claims the word "substantially" is used to described statically and dynamically balanced. For purpose of prior art searches the examiner will assume this implies the standard methods use to dynamically and statically balance any rotating object applies.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 52-57 59-63, 66, 68-69, 71-75, 78, 80-81, 83-84 and 89-92 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moos 5881152 A, and further in view of Anon, IBM TDB NN 85122861 and Evans US5445532 A.

7. As per claim 52, the limitation of a secure recording medium (i.e. storage medium) having at least one audio, video and software content is disclosed by Moos. Moos discloses a data storage device which may be magnetic, optical (optical storage devices would include a DVD), etc (see Column 2, lines 18-19) such that the data content of the storage media is encrypted and thus secure (Column 2, line 64). The storage device is equipped with a programmable memory chip which is provides a device for protecting stored data in data stored media (Column 1, 66-67 continuing top line of Column 2) and thus a disk security chip in the case of an optical disk. That the chip contains a security key is disclosed by Moos (Column 2, line 64-66). The data stored on these devices is encrypted with a different encryption key which servers distinguish different systems from one another (Column 2, line 38-40). The chip installed on the data storage medium can communicate with a computer (see Figure 2; Column 2, lines 53-55), and thus the computer must have a reader (player in the case of an optical disk) to read the information off the disk. Moos discloses that the chip does communicate with the computer (Figure 2 , 10 to 30) and further that the computer contains security software which runs on the computer side of the connection between the computer and the chip (column 2, lines 53-54). This would imply the existence of hardware (i.e. chip or chips) for the execution of such software but Moos is silent on the details. Moos is also silent on a first antenna connected to the chip on the optical

storage device and a second antenna connected to a player chip in the optical storage device reader (player). Nor does Moos disclose making the player chip detachable from the player.

8. Anon teaches communicating from a rotating storage media and logic assemblage to a stationary reader using an antenna located in the rotating frame of the storage media to an antenna located in a stationary reader (player) on at least one recording disk (that is *one* or more, see first line of disclosure). The antenna affixed to the rotating storage medium is connected to the logic assemblage consists of a layer of integrated electronic circuits using a semiconductor substrate and standard semiconductor fabrication techniques, such that the integrated circuit has memory, logic function, input/output and is able to carry out computations and thus functions as a processor (i.e. an embedded "chip"). The electronics on the rotating disk are coupled to external circuitry which allows them to exact power, and function as a data input/out port using wireless means, which according to the Anon could include transformer coupling, or capacitive or electro-optical. The diagram (page 2) illustrates wireless connection through two coils one fixed to the stator and one attached to the rotating disk. These coils serve as a first and second antennas, one connected to the embedded "chip" and to the external logic circuits which according to Anon's diagram, terminates in the read/write unit of Anon's system. Further, Anon teaches that the antenna should be connected directly to the chip in the case disk and further Anon terminates the communication links inside the player unit itself see diagram (x indication termination). Thus one of ordinary skill in the art at the time that the invention was made would have

been motivated to modified the teachings of Moos that a embedded chip is placed on a disk storage medium (including an optical disk) and further that at the same time that security software is executed in logic hardware (a chip) and communicates with the embedded chip with the teaching of Anon that antennas should be connected to both chips so that they can communicate and that the player chip that runs the security software on the hardware (IC) should be part of the player unit as indicated by Anon's figure and thus a player chip because Anon's antennas connected to chips would provided a wireless communications link that is not described in Moos.

9. The limitation to make the chip in the player is removable (detachable) is disclosed by Evans. Evans, realizing the need for removable (detachable) chips, teaches reusable chip sockets to per flexibility in maintenance, troubleshooting or replacement without risk of damage to the IC due to unnecessary heat (Column 1, lines 53-58). It would have been obvious for one of ordinary skill in the art at the time of that the invention was made to have modified the teachings of the combination of Moos and Anon with the teaching of Evans to provide for maintenance and upgrades to security protocols which would be burned on the chip. Claim 52 is rejected.

10. As per claim 53, the limitation of common content for two disk is disclosed by Moos Column 3, lines 31-33. Moos teaches the use of his invention for copy prevention (and hence copy protection) for digital content on his disk. Thus Moos teaches more than one disk having the same content as there is no need for copy protection if a single copy of the digital content suffices. Claim 53 is rejected.

11. As per claim 54, the limitation that the security key for audio and video content is different. Video and the correspond audio are general separately because of bandwidth differences and processing differences. Thus one of ordinary skill in the art at the time the invention was made would have been motivated to store these two digital contents separately (even through they are connected with the same creative work) because of the different file format and processing requirements. Further encryption under a different key would provide more security to the creative work. Claim 54 is rejected.

12. As per claim 55, the limitation that the DVD disk is "substantially" statically balanced with the meaning that substantially means using the methods and testing procedures of manufacturing to insure uniformity would apply. Since such is common business practice to insure quality and safety of the device then certain it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement such quality control to insure uniformity and safety. Claim 55 is rejected.

13. As per claim 56, the limitation that the that the DVD disk is "substantially" dynamically balanced with the meaning that substantially means using the methods and testing procedures of manufacturing to insure uniformity would apply. Since such is common business practice to insure quality and safety of the device then certain it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement such quality control to insure uniformity and safety. Claim 56 is rejected.

14. As per claim 57, the limitation that the player security chip decrypts data received from said disk "chip" . According to the teaching of Moos, the data is encrypted with

the secret key stored in the memory are of the disk "chip" (Column 2, lines 64-66). The data is decoded (decrypted) by the target system (the external computer Column 3, lines 6-14) using the security software of the target system (Column 3, lines 3-5) and hence is decrypted by the reader (or player) security chip. Claim 57 is rejected.

15. Claim 58 and 70 rejected under 35 U.S.C. 103(a) as being unpatentable over Moos 5881152 A, and Anon, IBM TDB NN 85122861 further in view of Olukotun et. al. The Case for a single-chip Multiprocessor (1996)

16. As per claim 58, and 70, the limitation that the cryptographic and authentication functions and the function DVD decoder (encoder) are performed together is disclosed by Moos (Column 1, lines 49-52; Column 2, line 46-47; Column 3, lines 1-3). Moos is silent on the actual combination of the cryptographic functions of the player chip and the compression/decompression properties of the DVD decoder (encoder) onto a single integrated monolithic chip.

17. Olukotun et. al. The Case for a Single-Chip Multiprocessor suggest with the new billion transistor chips that the placement of an entire system on a chip, that is multiple processors is superior to massive parallelism (see section 3, in particular page 3, Column 2 first and second paragraphs). And in particular greater processor speeds can be expected with multiple processors on a single chip. Placing the functions of decoding and decryption, together on a SOC would have been obvious to one of ordinary skill in the art at the time that the invention was made to have modified the teaching of Moos/Anon with the teaching of Olukotun et. al. SOC because of performance (on-chip activity can generally proceed faster than off-chip activity); power

(on-chip capacitances are mush lower than off-chip ones, so on-chip activity is more power-efficient); reliability inter-chip connections through PCBs are a significant source of unreliability, and there is less to go wrong if everything is on one chip); cost (provided the SOC is not uneconomically large it is cheaper than the equivalent multi-chip solution); size (small physical size (and weight) is an advantage for many application); and electromagnetic interference (emi) (because capacitance on chip are must lower, currents are lower and less radio interference is generated) which could also be an anvantage in low power wireless. Claim 58 and 70 are rejected.

18. Claim 58 and 70 rejected under 35 U.S.C. 103(a) as being unpatentable over Moos 5881152 A, and Anon, IBM TDB NN 85122861 further in view of Anderson et. al. Tamper Resistance-a Cautionary Note, 1996

19. As per claims 59-60, the limitation that the player security chip is generally tamper-resistance by Moos (Column 1, lines 6-8). Moos Specifically teaches about preventing (that is making tamper-resistance) and identifying tampering see Column 1, line 7, but is silent on the specifics as to how he will make the information inside the chip tamper resistance and how specifically the chip will identify when an attack is taking place. Anderson et. al. give a detail account of various attacks on chips(non-invasive attacks section 2.1; physical attacks section 2.2; reverse engineering 2.3 (cloning) and being section 2.5 method of protection in commercial systems especially) and reverse engineering for both military and commercial chips and methods of preventing such attacks. One of ordinary skill in the art at the time the invention was make would have been motivated to apply the standard methods of making chips

tamper resistance and resistance against reverse engineering (cloning) to implement Moos' "preventing or identifying tampering" Column 1, line 7 in the Moos/Anon invention. Claims 59-60 are rejected.

20. As per claims 61-62, the limitation that the player chip should be upgradeable or backward compatible. Moos is silent on whether his system is upgradeable or backward compatible, however one of ordinary skill in the art at the time the invention was made would have been motivated to have incorporated the capabilities of upgrading and making compatible changes to the system because as the system itself is upgrade due to changes in standards (e.g. MPEG) one would need to have these capabilities as a selling point for the system. Claims 61 and 62 rejected.

21. As per claim 63, the limitation that the player security chip performs authentication with the disk security chip is disclosed by Moos Column 2, lines29-32 lines 43-45. Claim 63 is rejected.

22. As per claim 66, the limitation disk security chip performs an authentication process with the player security chip. Moos disclose such authentication Column 2, line 43-45; Column 3, lines 1-3 and figure 2 units 20 and 30 constitute the player). Claim 66 rejected.

23. The limitation of claims 68-75, parallel the claims 52 and 57-63 in which the content of the storage medium is not restricted to audio, video or software. Thus the Moos/Anon/Evans would satisfy this broader limitations. Claims 68-75 are rejected.

24. Claim 78 is a method claim corresponding to device claim 52, with the added limitation that the disk key is not known to a disk manufacturer. The combination

Moos/Anon is silent with regards to who should known the keys, however, Moos is very emphatic preventing and identifying tampering to the disk chip and insuring that its content (i.e. key material) remain secret (Column 1, lines 7-8). One of ordinary skill in the art would at the time the invention was made would recognize that the disk manufacture does not have a need to know the key material on the chip in order to embed the chip in the disk and that it would become a security risk as the more people having access to that information the more liklihood that it would be compromized. Claim 78 is rejected.

25. As per claim 80, the limitation of encrypting the content of the disk with the disk key. Moos teaches encryption of the disk content in data storage area of the disk using keys stored in the embedded chip (Column 1, lines 41-42; 53-55). Claim 80 is rejected.

26. As per claim 81, the limitation of performing authentication between the player security chip and the disk security chip is disclosed by Moos Column 2, lines29-32 lines 43-45. Claim 81 is rejected.

27. As per claim 83, the limitation that after the disk security chip has verifying that the player is authentic, sends the player the disk key. Moos teaches validating the player (Figure 2 elements 20/30) Column 3, lines 7-12 (here authentication is through the symmetric key and challenge response), the disk chip sends a key that permits decoding (decryption). Claim 83 is rejected.

28. As per claim 84, the limitation that the disk chip sends the player the disk key encrypted by the player key is disclosed by Moos. Moos teaches that the chip contains the public key pair and the symmetric key (Column 2, lines 29-32). Further Moos

teaches that the *private* key of the public key pair is used to *encrypt* the digital data content stored on the disk (Column 2, lines 64-66), and hence the private key is the content key. The secret key of the symmetric key system is used for mutual authentication between the player and the disk chip (Column 3, lines 7-12) and in particular would be the player key as all user must have it in order to perform the authentication (Column 3, lines 3-5). The *public* key of the public key pair is then read from the disk chip and used to *decrypt* (decode) the content. It is inherent in this system that the public key must be kept secret and this is the reason why it is stored on the disk chip. It is inherent because if the public key were truly public then it could be used to by-pass the copy protection of the system. Thus it must be sent to the player to perform the decryption using the security software. But if it in sent in the open, again the system would be compromised, and hence it must be encrypted. Again the only key available to both parties is the symmetric key (player key) and hence the chip encrypts the public key using the player key and sends it to the player. Claim 84 is rejected.

29. As per claim 64, the play security chip verifies legitimacy of disk security chip by means of a function of a geometric property of the DVD. Litman teaches the use of geometry to authenticate and in particular items such as credit cards, smart cards, compact disks (Column 1, lines 30; Column 2, line 11)and further devices used in reading them such as compact disk player, CD-ROM drives, Floppy, optical or floptical disk drives (Column 1, lines 33-39). One of ordinary skill in the art at the time that the invention was made would have been motivated to modify the Moos /Anon system provides a simple solution to piracy and counterfeiting (Column 2, lines 13-21 Litman).

According to Litman, piracy and counterfeiting is costing the economy billions of dollars. Claim 64 is rejected.

30. As per claim 65, Moos and Anon are silent on the limitation that the geometric function depends on angle, diameter, thickness and eccentricity of the DVD. Litman teaches the use of geometric functions such as angle (Column 17, lines 32-34), dimensions of object (length, width, thickness, diameter) Column 7, lines 31-51, Litman, and finally eccentricity (which is defined in terms of terms of the major and minor diameters of an elliptical object and hence a function of dimensions). It would have been obvious for one of ordinary skill in the art at the time the invention was made, to combine the teaching of Moos and Anon with those of Litman because variation of geometry (angles, dimensions, etc.) is hard to copy when copying information onto a new disk. Variation of manufacturing insures this. Note here the angle here involves the layers of the disks rather than artificially introduced elements, but again due to variations in manufacturing techniques, the measurement of these also provides a unique identifier. Claim 65 is rejected.

31. The limitation of claims 76 and 77 are the same as claim 52 and dependent claim 63 combined and in claim 64 the limitation of eccentricity is dropped. Thus the Moos/Anon/Litman combination would also apply. Claims 76-77 are rejected.

32. As per claim 85, Moos and Anon are silent on the limitation of identifying (ID) and validating the disk key using a function of geometry of the disk Litman teaches using geometric feature such as angle, dimensions (including length, width, thickness, diameter, etc.) to identify and validation objects. It would have been obvious for one of

ordinary skill in the art at the time the invention was made, to combine the teaching of Moos and Anon with those of Litman because variation of geometry is hard to copy when copying information onto a new disk. Variation of manufacturing insures this. Further Moos teaches tamper proof storage (Column 1, line 7-8) hence tamper proof storage and variable manufacturing techniques insure that validation of the disk key can be performed in a unique way. Claim 85 is rejected.

33. As per claim 86, the limitation that the geometric property is the angle between layers is disclosed Column 17, lines 33-35. Note here the angle here involves the layers of the disks rather than artificially introduced elements, but again due to variations in manufacturing techniques, the measurement of these also provides a unique identifier. Claim 86 rejected.

34. As per claim 88, the limitation of a method for securing a DVD with a disk security chip connected to a first antenna disposed in the DVD and a second antenna connected to a player chip in the player (See Moos Column 2, and Anon lines 1-11; 20-23). The player security chip verifying the legitimacy of the disk by means of a function of geometry property of the DVD (Litman, Column 7). Claim 88 rejected.

35. Claims 64-65, 76-77, 85-86, 88 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moos/Anon as applied to claims 52-63 above, and further in view of Litman US 5988500 A.

36. Claims 67, 82 and 93 are rejected under 35 U.S.C. 103(a) as being unpatentable over the Moos/Anon/Litman combination as applied to claim 66 above, and further in view of Menzes et. al. Handbook of Applied Cryptography.

37. As per claim 67, the limitation that the authentication process is a zero-knowledge interaction. Menzes teaches Interactive zero-knowledge protocols pages 406-410. One of ordinary skill in the art at the time the invention was made, would have been motivated to modify the Moos/Anon/Litman combination with the interactive zero-knowledge proof because there is no leakage of information in either direction. Claim 67 is rejected.

38. As per claim 82, the limitation that the authentication process consists of mutual zero-knowledge interaction Menzes teaches Interactive zero-knowledge protocols pages 406-410. One of ordinary skill in the art at the time the invention was made, would have been motivated to modify the Moos/Anon combination with the interactive zero-knowledge proof because there is no leakage of information in either direction. Claim 82 is rejected.

39. As per claim 89, the limitation that a disk key K_d is programmed in each disk chip is disclosed by Moos Column lines 65-66. Claim 89 is rejected.

40. As per claim 90, the limitation that the disk key is specific to a particular disk of a plurality of disk is disclosed in Moos Column 2, lines 38-40, that the key was associated with a personalized data would indicate it would have to be different for each disk. Claim 90 is rejected.

41. As per claim 91, the limitation that each dsik chip is programmable after packaging in a commercial shipment package is disclosed in Moos Column 2, line 41. Moos notes that the chip is programmable (Column 2, line 1) and that it may be

personalized indicating that it may be programmed after packaging in a commercial shipment package. Claim 91 is rejected.

42. As per claim 92, the limitation wherein each disk chip is operative to check disk specific authorization. Moos discloses that the chip authenticates persons trying to access data, and hence determines if they have authorization to the data (Column 2, line 32). Claim 92 is rejected.

43. Claims 93-95 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moos/Anon combination as applied to claims 52 above, and further in view of Clark et. al. A Survey of Authentication Protocol, 17 November 1997.

44. As per claim 93, the limitation that after verifying the player authenticity, the security chip on the disk sends a disk key encrypted with a known player (disk reader) key. Moos is silent on how the content key K_c is sent to the player after the player is verified by disk. Menezes teaches Diffie-Hellman key exchange (page 515-516) and so after the validation of the player to the disk, a common key K can be established by Diffie-Hellman. Once a session key is established then the disk key K_d may be encrypted using the session and sent to the player. It would have been obvious for one of ordinary skill in the art at the time the invention was made to have share the disk key K_d with the player because this insures anything sent to the player by the disk can be validated by the player using a random number and a hash function. Claim 93 is rejected.

45. As per claims 94 and 95, the limitation that the player chip sends a random number R to the disk chip and the player chip encrypts the content key and hashes R

using a hash function f known to both the disk chip and the player chip K_c using the disk key K_d see Clark 6.1.5. It would have been obvious to one of ordinary skill in the art at the time the invention was made because by hashing R with f that is f(R) and concatenating this with the content key K_c and encrypting with K_d, the player knows that the content key did come from the disk as only player and the disk have the disk key and the player can hash R to see if it matches with what was sent to check that it was the disk that indeed sent it. Claims 94-95 are rejected.

Response to Arguments

Applicant's arguments filed 02 April 2004 have been fully considered but they are not persuasive.

46. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the discussion of the applicant pages 10 the structural differences in Anon and his invention as for example Anon first and second antennas. Anon was used to teach using antennas attached to chips as a means of communicating data from a logic chip on a rotating storage media to one on a stationary reader. Moos discloses the optical storage media. Further the differs in Moos cited at the bottom of page 10 and 12 are not claimed features.) are not recited in the rejected claim(s). Further Anon teaches at least one disk which would include the case of one disk, although Anon was not specially used to teach this feature. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

47. Applicant page 11 remarks that Moos lacks any suggestion of a player security chip. The examiner disagrees. The chip installed on the data storage medium can communicate with a computer external to the storage medium (Column 2, lines 53-55), and thus the computer must have a reader (player in the case of an optical disk) to read the information off the disk and communicate with the chip. Moos does state that the *computer* contains security software which must be executed on some processor or chip and the optimum location would be in the disk reader (column 2, lines 53-54 see above discussion for details), which further implies that there is a "security chip" on the reader side of the communication link to run security software.

48. With regards to the applicant statement at the bottom of page 13 that hardware upgrades are not an obvious modification to one of ordinary skill in the art, the examiner would call attention to the provision of Microsoft plug and play that hardware upgrades are indeed common and in fact needed for compatibility of older systems. For example chip sets for Bios upgrades with chip sets are very common.

49. With regards to the applicant statement on page 14, with regards to the to the integration of the player security chip integrated into a decoder circuit of the player, the placement of processes, such as decoding, security, read functions on separate chips is expensive and wasteful in the senses if these functions can be combined they are less expensive, faster, more, reliable, and power efficient, the examiner submits the article by Olukotun et. al. The Case for a Single-Chip Multiprocessor.

50. With regards to the request at the bottom of page 14 for a reference on tamper resistance of security chips the Examiner supplies a copy of Tamper Resistance –A Cautionary Note by Anderson and Kuhn.

51. With regards to applicant's statement at the top of page 15 concerning the limitation of claim 78, Moos recites nothing about the claimed limitation of "providing disk security chip and a disk key not known to a disk manufacturer" however, Moos makes it clear that he does not wish the contents of the disk (the key material material) to be compromised and indicates that he will take steps to prevent and identify such compromises (Column 1, lines 7-8). In the article by Anderson Tamper Resistance-A Cautionary Note) page 2 he notes that attacker fall into three classes—Class I clever outsiders, Class II knowledgeable insiders, and Class III funded organization. Of these the knowledgeable insider is the most threatening. Anderson notes that even Class III rely on them. They provide a treat because as insider they have access to knowledge that Class I and Class III do not possess. To prevent such a treat, the United States intelligence community has relied on the principle of "need to know" to prevent compromise of sensitive data. Certainly it would be recognized that the disk manufacture does not have a "need to know" the key material on the chip in order to embed the chip in the disk and that it would become a security risk as the more people having access to that information the more likelihood that it would be compromized. Further, there is no reason that the disk manufacturer would need to know anything about the disk if the chip is merely embedded as part of a manufacturing process.

52. With regards to the applicant's statement at the bottom of 15, with regards to claim 84 the applicant has not claimed a public key in any limitation of the claim. Further the applicant is referred to Moos that the *secret* (private part) of the *asymmetric key pair* is used to *encrypt* the digital content stored on the disk (Column 2, lines 64-66) and so it is clear that the public part is used to *decrypt* the encrypted data, in particular Moos states that "the data is encrypted with the secret (or private) part of the asymmetric key" (Column 2, line 64-65). According the public part of the asymmetric key must be used to decrypt the data. This is the nature of a public key system—one key of the key pair is used to encrypt the data the other is used to decrypt it. If the public key is used to decrypt, then it too must be kept secret. See discussion above.

53. The examiner has provided as requested references of the teaching that the applicant has asked for on tamper resistance; cloning of chips; "need to know" policy to prevent compromise of sensitive data; chip removal and replacement (such as upgrading bios chip sets on a mother board), as well as the case for consolidating different but related processes to a single-chip (Single-chip Multiprocessor).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

James Seal

James Seal
Examiner AU 2135
11 July 2004